Important Information about Scams & Frauds

Online Fraud is growing – Internet fraud can be any type of scheme/scam that uses the Internet – chat rooms, email, message boards or websites – to deceive prospective victims. As a Bank Customer, your need to be especially vigilant to some the frauds out there. Here are some types of Online Fraud:

Phishing – Fraudulent emails appearing to be from a trusted source such as your bank, or a government agency.

Defense Tactic:

If you receive an email that warns you, with little or no notice, that your account will be shut down unless you reconfirm certain information, DO NOT click on the email link. Instead call the company directly.

Before submitting any financial information to a legitimate website, look for the "lock" icon on the browser status bar, or look for the "https" in the web address. Both are indications that the information is secure and encrypted during transmission.

Spoofing – Web spoofing allows an attacker to create a "shadow copy" of any legitimate website.

Defense Tactic:

Be wary of unsolicited or unexpected emails from all sources.

If an unsolicited email arrives, treat it as you would a phishing source.

Identity Theft Frauds – This is where criminals obtained the names and social security numbers of their victims and use them to apply for credit cards and other items.

Defense Tactic:

Keep a close eye on your account activity at your bank. Report anything that looks suspicious.

Make sure your unused checks, bills, and statements are shredded before discarding.

Be careful about giving out Personal Data Online.

Review Credit Card and Account Statements.

Remember, your bank or a government agency will never send you an email asking you to disclose your personal information.